

See also: [PluginTOTP](#)

Two-Factor Authentication (2FA) is a security mechanism that requires users to provide two different authentication factors to verify their identity. This significantly enhances security by adding an extra layer of protection beyond just a password.

Starting with [Tiki 21](#), 2FA was introduced to strengthen the security of user accounts during authentication, helping to prevent [SIM Swap Scam](#).

Tiki uses [pragmarx/google2fa](#), a PHP implementation of two widely used algorithms for generating one-time passwords (OTPs) in 2FA systems:

TOTP (Time-based One-time Password) - open standard documented in [RFC 6238](#).

TOTP is similar to HOTP but incorporates a time factor.

- Algorithm: Based on HOTP
- Input: Secret key + Current timestamp
- Output: 6-8 digit numeric code
- Validity: Typically 30 seconds
- Use Case: Real-time applications requiring immediate validation.

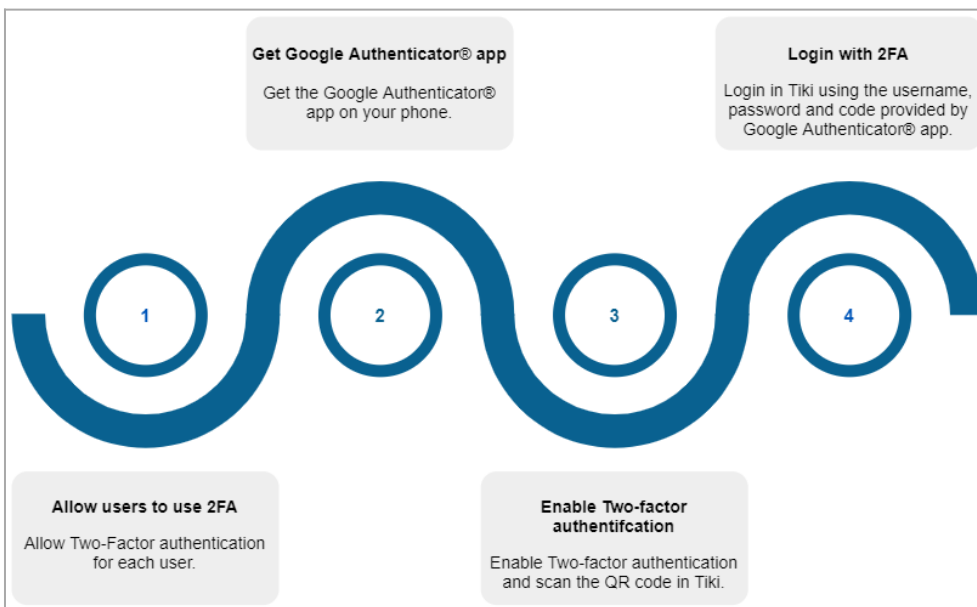
HOTP (HMAC-based One-time Password). - [RFC 4226](#)

HOTP generates a one-time password using a secret key and a counter.

- Algorithm: Based on HMAC-SHA1
- Input: Secret key + Counter value
- Output: 6-8 digit numeric code
- Validity: Until used (not time-dependent)
- Use Case: Ideal for systems where time synchronization isn't critical or possible

Tiki primarily uses TOTP, which offers several advantages:

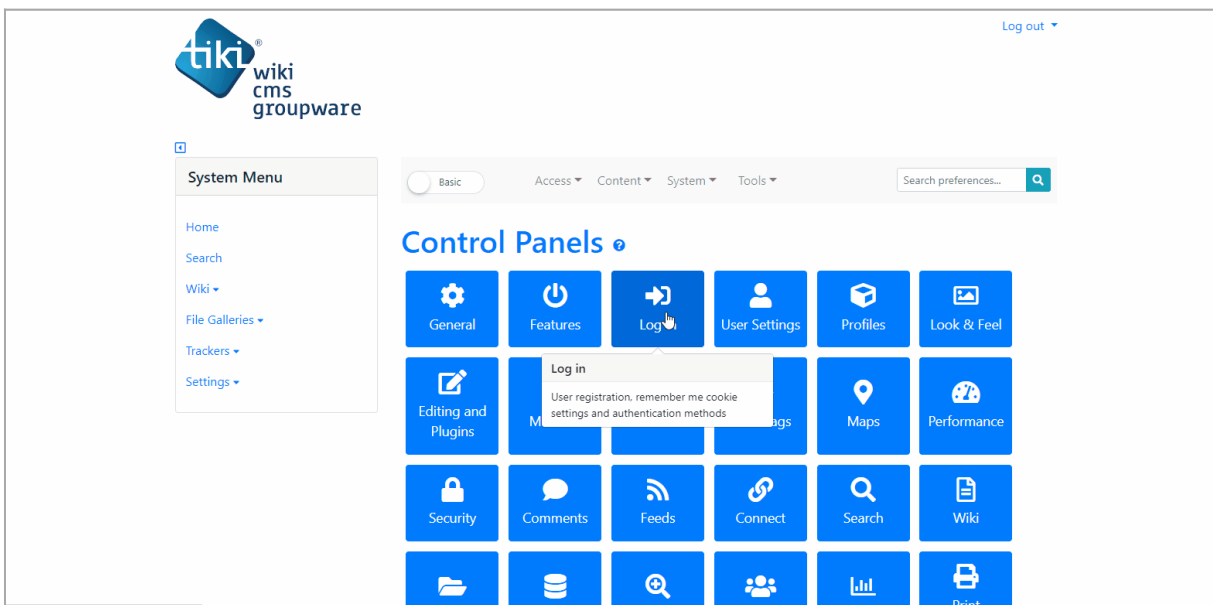
1. Enhanced Security: Protects against unauthorized access even if passwords are compromised.
2. Flexibility: TOTP adds an additional layer of security by being time-based
3. Cross-Platform Compatibility: Supported by a wide range of devices and applications.
4. User-Friendly: Easy to implement and use with mobile apps like Google Authenticator.
5. Compliance: Helps meet regulatory requirements for secure authentication.
6. And you can even use another Tiki instance via [PluginTOTP](#).



Click to expand

## Steps

**Step 1:** First enable the **Allow users to use 2FA** option in the "Log In" feature in your Tiki, go to **Settings** **Control Panels** **Log In** **General Preferences** tab **admin.php?page=login#contentadmin\_login-1** (e.g [http://www.example.com/tiki-admin.php?page=login#contentadmin\\_login-1](http://www.example.com/tiki-admin.php?page=login#contentadmin_login-1)) with **Preference Filters** to **Advanced**.



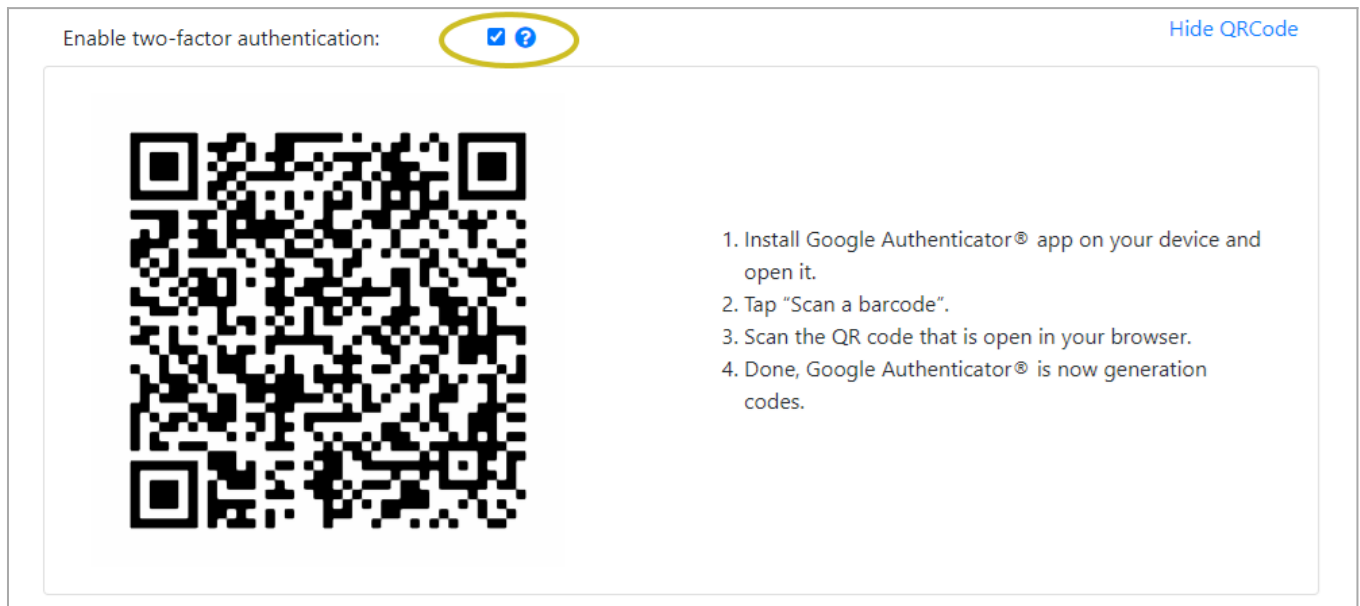
Click to expand

**Step 2:** Next, install Google Authenticator® App on your mobile phone. [See how to install it here.](#)

**Step 3:** Check the **Enable two-factor authentication** option in the **User Preferences** page, the **Account Information** tab and click on **Save changes** button. Note that the current password is required to make

changes.

At this step, you need to connect Tiki and the Google Authenticator application by scanning the QR Code generated in the `UserController::showQRCode()` page. Click on "Show QRCode" to display the QR Code, scan it using the application you installed in step 2.



Click to expand

**Step 4:** Finally, when authenticating on page "Log In" (e.g. `UserController::login()`), take the code generated by Google Authenticator App and enter it in the field `Two-factor Authenticator Code`.

**Log In**

Username:

Password:

[I forgot my password](#)

Two-factor Authenticator Code:

[Register](#)

Click to expand

By adhering to standardized algorithms like TOTP and HOTP, 2FA solutions become both secure and flexible. These methods make user authentication robust and effective.

## Related links

- Original commit: <http://sourceforge.net/p/tikiwiki/code/70793>

## Page aliases

---

- [2FA](#)